A STUDY ON CYBERCRIME PREVENTION AND INVESTIGATION IN INDIA WITH EMPHASIS ON ROLE OF AI

Synopsis of the Research Proposal

Submitted for the Registration in the Ph.

D. Programme (Part-Time) in Law

Submitted by:

Ankit Sharma

(Enrollment Number: 25JPPHDDLS002)

Under Supervi sion of

Dr. Tanmay Agrawal

(Assistant Professor)

ICFAI Law School

The ICFAI University, Jaipur

A Study on Cybercrime Prevention and Investigation in India with emphasis on role of AI

Synopsis of the Research Proposal

Submitted for the Registration in the Ph.

D. Programme (Part-Time) in Law

Submitted by:

Ankit Sharma

(Enrollment Number: 25JPPHDDLS002)

Under Supervision of

Dr. Tanmay Agrawal

(Assistant Professor)

ICFAI Law School

The ICFAI University, Jaipur

TABLE OF CONTENTS

S. No.	Contents	Page No.
1	Title/Abstract	4
2	Introduction	5
3	Review of Literature	7
4	Research Gap	10
5	Statement of Problem	10
6	Significance of The Study	11
7	Research Objectives	11
8	Research Questions	11
9	Research Hypotheses	12
10	Research Methodology	12
11	Scope and Limitations of the Study	14
12	Expected Outcome	14
13	Research Timeline	15
14	Reference	16

TITLE

A Study on Cybercrime Prevention and Investigation in India with emphasis on role of AI

ABSTRACT

The proliferation of technology can be seen in every industry. Artificial intelligence is one of the most prominent technological instruments being employed in almost all functional processes in the present day. In the modern world, which is driven by technology, the phrase artificial intelligence hereinafter referred as AI is gaining increasing relevance. In light of the challenges present in today's dynamic environment, AI continues to evolve as a developing field with vast potential and certain limitations. Artificial intelligence and the concept of cybercrime, which is closely associated with it, are becoming increasingly prevalent. With rapid technological advancement, cybercrimes are being committed at an alarming rate, and the use of sophisticated digital tools often amplifies their impact rather than limiting the consequences. However, the increasing prevalence of AI-driven cybercrimes presents a serious challenge to law enforcement and legal frameworks. Existing cybercrime laws, such as the Information Technology Act of 2000, Bhartiya Nyaya Sanhita, 2023, Bhartiya Sakshya Adhiniyam, 2023 were not designed to address the complexities and nuances of AI-enabled offenses. There is a lack of comprehensive legislation that adequately covers the intersection of AI and cybercrime, leading to difficulties in prosecuting offenders, handling digital evidence, and securing data. This research aims to examine the conceptual and legal dimensions of artificial intelligence and cybercrime in India, along with a comparative international perspective. It further seeks to analyse the adequacy of existing legal frameworks in addressing AI-driven cyber threats and the challenges faced by investigative agencies. The study identifies key gaps in the current cybercrime prevention mechanisms, including issues such as the rapid evolution of AI technologies, the difficulty in tracing AI-based crimes, and the inadequacies of the existing digital forensics tools. The proposed solutions emphasize the need for international cooperation, continuous updates to legislation, and enhanced training for law enforcement to keep pace with technological advancements.

Keywords: Artificial Intelligence, Cyber security, Legal Framework, Data Protection, Digital forensics tools, prevention, investigation.

1. INTRODUCTION

Technology is now an essential component in many aspects of life, including the working world and the living world. Within the realm of technology that we live in today, the term "artificial intelligence" is used rather often. At this point in time, it is still a science that is in the process of evolving in many respects. AI has been able to establish its relevance in everyday life, from the resolution of difficult problems to the suggestion of material and the provision of virtual support. The term "cybercrime" refers to a kind of criminal activity that is carried out via the use of the internet, technology, and artificial intelligence that has been established relatively recently. The use of artificial intelligence to fight cybercrimes is becoming more necessary in conjunction with the promotion of cyber security. In this research, an attempt is made to investigate the role that artificial intelligence plays in reducing cybercrime from both an Indian and an international point of view.[1]

The use of 'artificial intelligence has already been' implemented in a wide variety 'of applications' with the goals of boosting productivity, enhancing sales, or improving experiences. Nevertheless, the primary emphasis of this paper is on a significant use of artificial intelligence that is sometimes disregarded: the enhancement of defence against cyber attacks. Artificial intelligence is a potent tool for guarding against cyber security assaults when it is used in combination with conventional approaches.[2]

Cisco, on its own, revealed that in 2018, they stopped seven trillion attacks on behalf of its clients. These figures are really amazing. Given the ever-increasing nature of the risks, companies need assistance. Some companies are looking to artificial intelligence, not so much to entirely solve their issues yet, but rather to strengthen their defences against potential threats. "Organizations are looking for automation, machine learning, and artificial intelligence to help make cyber security more manageable, more efficient, more effective, and lower their risk," says Martin Borrett, a distinguished engineer at IBM, chief technology officer at IBM, and technical executive for IBM's European security business unit. A smart phone has become an indispensable component of contemporary life, as shown by the fact that even those who are illiterate now use smartphone devices. When someone asserts that individuals in this day and age "live on the internet," they are not joking around. The use of the internet has steadily

[1] Singh, Rang. (2023). The Use Of Artificial Intelligence To Control Cyber Crimes In India: An Overview. ShodhKosh: Journal of Visual and Performing Arts. 4. 10.29121/shodhkosh. v4.i2.2023.2418.

[2] Kumar, N. (2025). The Role of Artificial Intelligence in Criminal Investigations in India. *Journal of Legal Studies "VasileGoldiş"*, *35*(49), 98-111.

become an essential component of day-to-day living. Everyone makes use of artificial intelligence in their day-to-day lives, but they lack the understanding and comprehension that is required.

Right now, hackers have a tremendous chance to easily fool people into believing something that is not true. Hackers may sometimes deceive folks who have a thorough knowledge of artificial intelligence. Cyberattacks are rapidly rising, despite the fact that effective security measures are in place. The malicious software, phishing, password attacks, drive-by downloads made possible via hyperlinks, virus attacks, and other forms of cyberattacks are all potential manifestations of this threat.

Cybercrime refers to a range of illegal activities that are committed using the internet or other forms of digital communication. These crimes can take many different forms and can have serious consequences for victims, including financial losses, damage to reputation, and emotional trauma. Some common types of cybercrime include:

- Hacking: illicit entry into a computer system or network to appropriate confidential information or inflict damage.
- Identity theft: the illicit use of an individual's personal information, such their Social Security number or credit card details, to perpetrate fraud.
- Cyber stalking: use the internet or other digital platforms to harass, intimidate, or threaten an individual.
- Cyber bullying: use digital methods to intimidate, degrade, or menace an individual, often a minor.
- Financial fraud: using the internet or digital communication to perpetrate fraud against others for monetary gain, including phishing schemes or counterfeit investment opportunities.
- Malware and virus attacks: The proliferation of malicious software, including viruses and ransomware, capable of damaging systems or exfiltrating critical information.

Cybercrime is a rapidly evolving area of crime that presents new challenges for law enforcement and society as a whole. The anonymity of the internet and the global reach of

digital communication make it easier for criminals to commit cybercrime and harder for authorities to track them down.

2. REVIEW OF LITERATURE

Stanford University (2025)[3] said that AI-related security incidents had risen to 233 in 2024, a 56% increase over 2023, and stated that cybersecurity was among the top three dangers for firms utilizing AI. It also found a considerable gap between understanding of AI hazards and the existence of effective protections, underscoring the need for further security measures.

University of Oxford and World Economic Forum (2025)[4] researched potential cyber vulnerabilities related with AI and identified concerns such as AI system manipulation, data poisoning and autonomous attacking systems. Their paper stressed the need of a risk-based approach to AI governance and suggested including cybersecurity safeguards throughout the AI lifecycle.

University of Oxford (2023)[5]**,** in its report the Malicious application of Artificial Intelligence: Forecasting, Prevention, and Mitigation, looked into the malicious application of AI, including automated hacking, deepfake fraud, and large-scale social engineering. The research coined the term "threat multiplier" for AI, showing how technology might increase the magnitude, speed and complexity of cyber attacks.

Lukosiute et al. (2026)[6]looked at how cybercrime affects the economy throughout the globe in respect to the risks presented by AI. The research showed that cybercrime costs the world hundreds of billions of dollars every year. Artificial intelligence could make these losses even worse, which shows how important it is to create stronger global rules.

Trinh (2025)[7]looked at how to group cybercriminals and the types of conduct they show via case study analysis. The researchers who did the study came to the conclusion that cybercrimes have different goals and techniques, which means that the law and investigations need to respond in different ways to deal with the expanding dangers.

[3] Stanford University. (2025). AI Index Report 2025.
[4] University of Oxford, & World Economic Forum. (2025). AI and Cyber Risk Report.
[5] University of Oxford. (2023). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation
[6]Lukošiūtė, K., Halstead, J., &Righetti, L. (2026). Global Cybercrime Damages: A Baseline for Frontier AI Risk Assessment. arXiv preprint arXiv:2603.20570.
[7]Trinh, V. D. (2025). Vietnam's Securitisation of Cybersecurity Under the Influence of a Rising China. *Australian Journal of International Affairs*, *79*(1), 169-188.

Dwivedi and Ranjan (2024)[8]looked examined how quickly cybercrime is growing in India in light of more people becoming online and more things becoming digital. discovered that cybercrime is increasing. According to the study's results, hackers use flaws in digital infrastructure to do things like phishing, stealing identities, and committing fraud online. Because of this, consumers' personal information and money are at danger.

Kaur, M., Saini, M. (2023),[9] Cyberbullying across various social media platforms is an escalating issue in today's technologically enabled society, endangering youth. The troubling incidence of cyberbullying rises annually, with catastrophic consequences. The Indian government has addressed this online threat by creating cyber cells, many hotlines (especially for women and children), complaint boxes, and rigorous legal procedures to deter and penalize cybercrimes. This research evaluates the relevant initiatives. A survey is conducted to enhance understanding of cyberbullying on college and university campuses. The poll addresses many factors contributing to cyberbullying among adolescents and proposes potential solutions to this issue.

P.B. Ajoy (2022),[10] The prevalence of cybercrimes and its adverse consequences have compelled several nations to enact laws to tackle the problem. Despite the enactment of legislation to fight it, cybercrime is increasing, as shown by the available statistics. The criminal justice system is inadequate in addressing cybercrime for many reasons. Factors include jurisdictional issues, extradition challenges, inefficiencies in law enforcement, difficulties in identifying, locating, and apprehending cybercriminals, a shortage of experts, technological obstacles, complications with international law, and issues related to cybercrime data, including underreporting. It is essential to focus on preventative measures against cybercrime, since current criminal legislation is insufficient to handle this issue effectively.

Misra, A., & Chacko, M., (2021),[11] Hacks, ransomware attacks, and other cybersecurity breaches are more common in India despite the country having one of the world's biggest software personnel infrastructures. Due to the absence of a unified cybersecurity framework,

---

[8]Ranjan, R. (2024). EVOLVING LEGAL LANDSCAPE: ISSUES AND INSIGHTS IN MODERN JURISPRUDENCE. The Law Way With Lawyers.

[9]Kaur, M., Saini, M. (2023), Indian government initiatives on cyberbullying: A case study on cyberbullying in Indian higher education institutions. *EducInfTechnol* 28, 581–615. https://doi.org/10.1007/s10639-022-11168-4

[10]Ajoy P.B (2022). Effectiveness of Criminal Law in Tackling Cybercrime: A Critical Analysis. SchInt J Law Crime Justice, 5(2): 74-79.

[11]Misra, A., Chacko, M. (2021), Square pegs, round holes, and Indian cybersecurity laws. *Int. Cybersecur. Law Rev.* 2, 57–64. https://doi.org/10.1365/s43439-021-00026-7

several sectoral legislation and criminal codes interact in an often-bewildering way, leading to substantial uncertainty. The purpose of this article is to survey the many statutes, rules, and policies that make up India's cybersecurity framework and to point out problems that stem from this disjointed approach.

Kshetri, (2020)[12]we carried out empirical research to investigate the connection between the protection of personal data and the commission of cybercrime. According to the findings of the research, the personal information of people is susceptible to cybercrime, and companies are required to take precautions in order to effectively safeguard this information.

Kim & Lee (2019)[13]carried out an empirical investigation with the purpose of developing a framework for the prevention of cybercrime. Based on the findings of the research, it was determined that a complete strategy for avoiding cybercrime should include legal, organizational, and technological measures.

Chen & Huang, (2019)[14] performed a thorough evaluation of the literature about cybercrime prevention via technology and education. The authors determined that technology and education are essential in mitigating cybercrime, and that an integrated strategy including technology, education, and legal frameworks is vital for successful prevention.

Bhatia & Kumar, (2018)[15]conducted a literature study on the topic of cybercrime and the prevention of it. The authors came to the conclusion that cybercrime is a rising concern, and that it is vital to have effective technological, legal, and organizational measures in place to prevent cybercrime and protect persons and organizations from the repercussions of cybercrime.

Kshetri, (2017)[16] executed an empirical investigation on cybercrime and the safeguarding of personal information. The research revealed that people and businesses often encounter privacy issues in the digital realm and determined that the advancement of privacy-enhancing technology and regulations may alleviate privacy hazards linked to criminality.

---

[12]Kshetri, N. (2020). Cybercrime and cybersecurity in India: Policy, challenges and solutions. Strategic Analysis, 42(1), 1-16.

[13]Kim, J., & Lee, D. (2019). "A framework for preventing cybercrime: An empirical study", Information Management & Computer Security, 27(4), 456-471.

[14] Chen, K., & Huang, H. (2019). "Cybercrime prevention through technology and education: A systematic review", Journal of Computer Information Systems, 59(3), 31-41.

[15]Bhatia, K., & Kumar, A. (2018). "Cybercrime and its prevention: A review of the literature", Journal of Cybersecurity, 4(2), 98-109.

[16]Kshetri, N. (2017). "Cybercrime and the protection of personal information: An empirical study", Journal of Management Information Systems, 34(1), 205-233.

D'Ovidio& Poggi's, (2016)[17]Analyze the many forms of cybercrime that have an effect on companies, such as cyberattacks, data breaches, and identity theft, and investigate the effects that cybercrime has on the operations of organizations, their reputations, and their financial performance.

3. RESEARCH GAP

1. AI's role in criminal investigations is not fully addressed by current legislation,
2. creating a gap in regulatory frameworks.
3. Existing privacy laws fail to adequately protect individuals from the risks posed by AI technologies in criminal activities.
4. Investigative methods and training are not evolving at the same pace as AI advancements, hindering effective response to AI-driven crimes.

4. STATEMENT OF THE RESEARCH PROBLEM

With the rapid advancement of Artificial Intelligence, criminals are increasingly leveraging technology to commit hard-to-trace crimes. However, the criminal justice system, comprising investigating authorities, law enforcement personnel, and legal professionals, often lacks the requisite expertise and technological competence to effectively counter these evolving threats. This mismatch creates significant gaps in timely investigation, evidence analysis, and ultimately, the delivery of justice.

Moreover, the accelerated integration of Artificial Intelligence into various aspects of criminal activity and investigation has outpaced the development of appropriate legal frameworks. The absence of robust legislative regulations and ethical guidelines governing the use of AI in criminal investigations raises serious concerns regarding individual rights, dataprivacy, transparency, and accountability. These challenges underline the urgent need for a comprehensive legal and policy approach to ensure the responsible and effective use of AI in the criminal justice system, while upholding constitutional safeguards and procedural fairness.

5. SIGNIFICANCE OF THE STUDY

[17]D'Ovidio, R., & Poggi, A. (2016). “Cybercrime and its impact on business”, Journal of Financial Crime, 23(3), 711-721.

It is now required to examine criminal conduct in order to discover the truth and to use artificial intelligence in order to quickly arrest criminals. This is because criminal activity is growing in the 21st century, and it is now important to study criminal behavior. The purpose of this action is to guarantee that the victim will be able to get justice and that society as a whole will be able to live in a more secure environment. A further advantage of artificial intelligence is that the evidence it generates is more precise and has the potential to affect the perspectives of humans. As a consequence of this, the organizations that are dealing with criminal investigations are required to get the particular training at this time. Additionally, the purpose of this study is to explore the role that artificial intelligence plays in the subject of forensic analysis.

6. RESEARCH OBJECTIVES

1. To attain the purpose of the research, the following objectives have been set forth:
2. To explore frameworks for assigning accountability in cases involving cybercrimes and AI breaches.
3. To explore the relevance and emerging challenges associated with prevention and investigation of cybercrime in era of AI.
4. To examine the role of artificial intelligence in the escalation cybercrimes.
5. To compare the various legislative framework across different jurisdictions of AI in cybercrime prevention and investigation.
6. To evaluate the judicial interpretation and approaches adopted by higher courts regarding AI and cybercrime.
7. To provide recommendations regarding current statutes to prevent escalation of cybercrimes in emerging AI era.

7. RESEARCH QUESTIONS

1. What is the framework of cybercrime and breaches in relation to its accountability?
2. What are the major challenges faced by law enforcement agencies in the prevention and investigation of cybercrimes in the era of Artificial Intelligence?
3. How does Artificial Intelligence contribute to the evolution and sophistication of cybercrimes?
4. What are the best practices in different territorial jurisdiction with respect to AI and cybercrimes prevention and investigation?

5. How and to what extent higher courts adapted existing legal principle to address emerging issues of cybercrime involving AI.
6. What statutory reforms are required to regulate the misuse of AI in cybercrime while balancing innovation and legal accountability?

8. RESEARCH HYPOTHESIS

For the present study the following hypotheses have been formulated:

- H1: The existing legal framework in India is inadequate to ensure effective accountability for AI related cybercrimes.
- H2: Artificial Intelligence significantly impacts the nature, investigation and regulation of cybercrime.
- H3: The Indian legal system lacks framework for liability of AI and damage computation mechanism in cases of AI and cybercrimes.

9. RESEARCH METHODOLOGY

The present study will adopt mixed research methodology which combines empirical and doctrinal research method. This method is appropriate as the research focuses on examining the existing legal framework governing cybercrime and the emerging role of artificial intelligence within it. The research relies extensively on secondary sources of data, including statutory enactments such as the Information Technology Act, 2000, relevant provisions of BNS, BNSS, BSA, and Digital personal Data protection Act, 2023 and other allied laws governing cyber offences in India. In addition, international legal instruments, conventions, and model laws relating to cybercrime and artificial intelligence are examined to provide a comparative perspective. Judicial pronouncements from Indian courts, as well as select foreign judgments, are analysed to understand the evolving judicial approach toward cybercrime and the use of AI in investigation and prevention.

The present research work also undertakes a critical review of legal literature, including ‘books, peer-reviewed journal articles, law commission reports, policy’ documents, government reports, and publications by international organizations. These sources help in identifying the

conceptual foundations, emerging trends, and challenges associated with AI-driven cybercrime.

The present study will adopt mixed research methodology which combines empirical and doctrinal research method. This method is appropriate as the research focuses on examining the existing legal framework governing cybercrime and the emerging role of artificial intelligence within it.

The research relies extensively on secondary sources of data, including statutory enactments such as the Information Technology Act, 2000, relevant provisions of BNS, BNSS, BSA, and Digital personal Data protection Act, 2023 and other allied laws governing cyber offences in India. In addition, international legal instruments, conventions, and model laws relating to cybercrime and artificial intelligence are examined to provide a comparative perspective. Judicial pronouncements from Indian courts, as well as select foreign judgments, are analysed to understand the evolving judicial approach toward cybercrime and the use of AI in investigation and prevention.

The present research work also undertakes a critical review of legal literature, including 'books, peer-reviewed journal articles, law commission reports, policy' documents, government reports, and publications by international organizations. These sources help in identifying the conceptual foundations, emerging trends, and challenges associated with AI-driven cybercrime.

For the empirical component of our study on the "Cybercrime Prevention and Investigation in India with emphasis on the role of AI," the following stakeholders will be targeted for empirical part of our research:

Primary stakeholders – AI developers and engineers, Cybersecurity professionals, Law enforcement agencies, victims of AI enable crimes, Legal practitioners.

Adjudicatory and Judicial Bodies – Courts and Tribunals that interpret Cyber laws and enforce responsibility.

Government & Regulatory Authorities – Bodies involved in policy-making and cybersecurity regulations.

Academic and Research stakeholders- University professors, phd Scholars and Academic bodies, Research institutions and Think tanks.

Civil society and End Users- General public using internet, NGOs working on privacy and cyber awareness.

10. SCOPE AND LIMITATIONS OF THE STUDY

SCOPE

This research examines the legislative framework in India that has been established to control and investigate cybercrime. It further explores various forms of cybercrime, including deep fakes, automated scams, and sophisticated cyber-attacks, while analysing 'the role of artificial intelligence in' shaping 'and' facilitating these offences. The study incorporates insights from legal stakeholders by engaging with existing laws, judicial precedents, and policy developments. Additionally, it adopts a comparative perspective by analysing norms and practices across multiple jurisdictions, 'including the United States, the United Kingdom, the European Union, Japan, and China', in order to provide a comprehensive understanding of global approaches to cybercrime regulation in the age of artificial intelligence.

LIMITATIONS

The study is subject to certain limitations. It has geographic constraints, as it relies on real-world data collected from a single location, which may not be fully representative of the entire country. Furthermore, these discoveries may become obsolete over time owing to the fast advancement of artificial intelligence and associated technologies. The research also faces challenges in accessing cybercrime investigation records and confidential information, which may affect the completeness of the analysis. Furthermore, certain aspects of the study depend on secondary sources, which may be limited in scope or potentially biased, thereby affecting the overall reliability of the findings.

11. EXPECTED OUTCOMES OF YOUR STUDY

1. The study will provide a comprehensive assessment of the adequacy and effectiveness of existing Indian laws in addressing AI-driven cybercrimes.

2. It will highlight key deficiencies, ambiguities, and challenges within the current cybercrime prevention and investigation mechanisms.

3. The research will clarify the dual role of artificial intelligence as both a tool for committing cybercrimes and a mechanism for their prevention and detection.

4. The study will propose practical reforms and policy suggestions to strengthen cyber laws and improve investigative frameworks in the era of artificial intelligence.

12.RESEARCH TIMELINE

Phase	Months	Targets
1	1-6 months (Year 1)	The conclusion of the study topic and objectives. A thorough examination of the current literature on artificial intelligence and cybercrime law. Putting together a plan for the research. Tools for research, such questionnaires and interview schedules, and how to develop them. This procedure includes finding important legal issues and getting first information from statutes, case law, and reports.
2	7-12 months (Year 1)	Analysis of judicial responses, case laws, and enforcement mechanisms in India
3	13-18 months (Year 2)	Interpretation and Analysis of data collected, Compilation of material, and report writing
4	19-24 months (Year 2)	Complete the Conclusion & Suggestions with the Recommendations. Final editing and proofing of thesis with Plagiarism checked certificate. Submission of Research Thesis and prepare for viva voce.

13. REFERENCE

- Ajoy P.B (2022). Effectiveness of Criminal Law in Tackling Cybercrime: A Critical Analysis. SchInt J Law Crime Justice, 5(2): 74-79.
- ‘Bhatia, K., & Kumar, A.’ (201 5). “Cybercrime: Types, laws, and preventions”, ‘Cybersecurity and Privacy, (pp. 1’ -1 3). Springer.
- ‘Bhatia, K., & Kumar, A.’ (201 8). “Cybercrime and its prevention: A review of the literature”, ‘Journal of Cybersecurity, 4(2), 98-‘1 09.
- ‘Chen, K., & Huang, H.’ (201 9). “Cybercrime prevention through technology and education: A systematic review”, ‘’Journal of Computer Information Systems, 59(3), 31 -41 ‘
- ‘D'Ovidio, R., & Poggi, A.’ (201 6). “Cybercrime and its impact on business”, ‘Journal of Financial Crime, 23(3)’, 71 1 -721 .
- ‘Kaur, M., Saini, M. (2023), Indian government initiatives on cyberbullying: A case study on cyberbullying in Indian higher education institutions.’ EducInfTechnol 28, 581 –61 5. https://doi.org/1 0.1 007/s1 0639-022-1 1 1 68-4.
- ‘Kim, J., & Lee, D.’ (201 9). “A framework for preventing cybercrime: An empirical study”, ‘Information Management & Computer Security, 27(4), 456-471 ‘.
- ‘Kumar, N. (2025). The Role of Artificial Intelligence in Criminal Investigations in India. Journal of Legal Studies’ “VasileGoldiş”, 35(49), 98-1 1 1 .
- Kshetri, N. (2020). Cybercrime and cybersecurity in India: Policy, challenges and solutions. Strategic Analysis, 42(1), 1 -1 6.
- Lukošiūtė, K., Halstead, J., &Righetti, L. (2026). Global Cybercrime Damages: A Baseline for Frontier AI Risk Assessment. arXiv preprint arXiv:2603.20570.
- Misra, A., Chacko, M. (2021), Square pegs, round holes, and Indian cybersecurity laws. Int. Cybersecur. Law Rev. 2, 57–64. https://doi.org/1 0.1 365/s43439-021 -00026-7.

- Singh, Rang. (2023). The Use Of Artificial Intelligence To Control Cyber Crimes In India: An Overview. ShodhKosh: Journal of Visual and Performing Arts. 4. 1 0.291 21 /shodhkosh. v4.i2.2023.241 8.
- Staniford, S., Webb, V., & Beech, A. (201 2). "The anatomy of a large-scale hypertextual Web search engine", Computer Networks, 56(1 8), 3825-3833.
- Trinh, V. D. (2025). Vietnam's Securitisation of Cybersecurity Under the Influence of a Rising China. Australian Journal of International Affairs, 79(1), 1 69-1 88.